Bases for qudits from a nonstandard approach to SU(2)

Maurice Robert Kibler

Bases for qudits from a nonstandard approach to $SU(2)$

Maurice R. Kibler[1]

[1a] *Université de Lyon, F–69622, Lyon, France*

[b] *Université Claude Bernard Lyon 1, Villeurbanne, France*

[c] *CNRS/IN2P3, Institut de Physique Nucléaire de Lyon, France*

Bases of finite-dimensional Hilbert spaces (in dimension d) of relevance for quantum information and quantum computation are constructed from angular momentum theory and $su(2)$ Lie algebraic methods. We report on a formula for deriving in one step the $(1+p)p$ qupits (i.e., qudits with $d = p$ a prime integer) of a complete set of $1 + p$ mutually unbiased bases in $\mathbf{C}^p$. Repeated application of the formula can be used for generating mutually unbiased bases in $\mathbf{C}^d$ with $d = p^e$ $(e \geq 2)$ a power of a prime integer. A connection between mutually unbiased bases and the unitary group $SU(d)$ is briefly discussed in the case $d = p^e$.

PACS numbers: 03.65.Fd, 03.65.Ta, 03.65.Ud, 03.67.-a, 02.20.Qs

I. PROLEGOMENA

The use of symmetry adapted functions (or state vectors) is of paramount importance in molecular physics and condensed matter physics as well as in the clustering phenomenon of nuclei. For instance, wavefunctions adapted to a finite subgroup of $SU(2)$ turn out to be very useful in crystal- and ligand-field theory [1]-[11].

It is the purpose of the present work to report on state vectors adapted to the cyclic subgroup C_d of $SO(3) \sim SU(2)/Z_2$. Such vectors give rise to bases of $SU(2)$, the so-called mutually unbiased bases (MUBs), to be defined in Section V. They play a fundamental role in quantum information and quantum computation in view of the fact that these bases describe

---

[1] From a talk presented at the 13th International Conference on Symmetry Methods in Physics (Dubna, Russia, 6-9 July 2009) organized in memory of Prof. Yurii Fedorovich Smirnov by the Bogoliubov Laboratory of Theoretical Physics of the JINR (Russia) and the ICAS at Yerevan State University (Armenia).

qudits (the analogs of qubits in dimension d). A single formula for MUBs is obtained in this paper from a polar decomposition of $SU(2)$ and analysed in terms of quantum quadratic discrete Fourier transforms, Hadamard matrices, generalized quadratic Gauss sums, and special unitary groups $SU(d)$.

Before dealing with the main body of this work, we continue this introduction with a brief survey for nonspecialists of some particular aspects of quantum computation and quantum information for which the concept of MUBs is useful.

According to the law by Moore, the size of electronic and spintronic devices for a classical computer should approach 10 nm in 2018-2020, i.e., the scale where quantum effects are visible, a fact in favor of a quantum computer. This explains the growing interest for a new field, viz., the field of quantum information and quantum computation. Such a field, which started in the 1980's, is at the crossroads of quantum mechanics, discrete mathematics and informatics with the aim of building a quantum computer. We note in passing that, even in the case where the aim would not be reached, physics, mathematics, informatics and engineering will greatly benefit from the enormous amount of works along this line.

In a quantum computer, classical bits (0 and 1) are replaced by quantum bits or qubits (that interpolate in some sense between 0 and 1). A qubit is a vector $|\phi\rangle$ in the two-dimensional Hilbert space $\mathbf{C}^2$:

$$|\phi\rangle = x|0\rangle + y|1\rangle, \quad x \in \mathbf{C}, \quad y \in \mathbf{C}, \quad |x|^2 + |y|^2 = 1, \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the elements of an orthonormal basis in this space. The result of a measurement of $|\phi\rangle$ is not deterministic since it gives $|0\rangle$ or $|1\rangle$ with the probability $|x|^2$ or $|y|^2$, respectively. The consideration of N qubits leads to work in the 2^N-dimensional Hilbert space $\mathbf{C}^{2^N}$. Note that the notion of qubit, corresponding to $\mathbf{C}^2$, is a particular case of the one of qudit, corresponding to $\mathbf{C}^d$ (d not necessarily in the form 2^N). A system of N qudits is associated with the Hilbert space $\mathbf{C}^{d^N}$. In this connection, the techniques developed for finite-dimensional Hilbert spaces are of paramount importance in quantum computation and quantum calculation.

From a formal point of view, a quantum computer can be considered as a set of qubits, the state of which can be (controlled and) manipulated via unitary transformations. These transformations correspond to the product of elementary unitary operators called quantum gates acting on one or two qubits. Measurement of the qubits outcoming from a circuit of quantum gates yields the result of a (quantum) computation. In other words, a realization of quantum information processing can be performed by preparing a quantum system in a quantum state, then submitting this state to a unitary transformation and, finally, reading the outcome from a measurement.

Unitary operator bases in $\mathbf{C}^d$ are of pivotal importance for quantum information and quantum computation as well as for quantum mechanics in general. The interest for unitary operator bases started with the seminal work by Schwinger [12]. Among such bases, MUBs play a key role in quantum information and quantum computation [13]-[17]. From a very general point of view, MUBs are closely connected to the principle of complementarity introduced by Bohr in the early days of quantum mechanics. This principle, quite familiar in terms of observables like position and momentum, tells that for two noncommuting observables, if we have a complete knowledge of one observable, then we have a total uncertainty of the other. Equation (41) in Section V for $a \neq b$ indicates that the development in the basis B_a of any vector of the basis B_b is such that each vector of B_a appears in the development with the probability $1/d$. This is especially interesting when translated in terms of measurements, the bases B_a and B_b corresponding to the (nondegenerate) eigenvectors of two noncommuting observables.

II. A NONSTANDARD BASIS FOR $SU(2)$

The various irreducible representation classes of the group $SU(2)$ are characterized by a label j with $2j \in \mathbf{N}$. The standard irreducible matrix representation associated with j is spanned by the irreducible tensorial set

$$B_{2j+1} = \{|j, m\rangle : m = j, j-1, \ldots, -j\}, \tag{2}$$

where the vector $|j, m\rangle$ is a common eigenvector of the Casimir operator j^2 and of the Cartan operator j_z of the Lie algebra $su(2)$ of $SU(2)$. More precisely, we have the relations

$$j^2|j, m\rangle = j(j+1)|j, m\rangle, \quad j_z|j, m\rangle = m|j, m\rangle, \tag{3}$$

which are familiar in angular momentum theory. (We use lower case letters for operators and capital letters for matrices so that j^2 in (3) stands for the square of a generalized angular momentum.)

Following the works in [18, 19], let us define the linear operators v_{ra} and h by

$$v_{ra} = e^{i2\pi jr}|j,-j\rangle\langle j,j| + \sum_{m=-j}^{j-1} q^{(j-m)a}|j,m+1\rangle\langle j,m| \tag{4}$$

and

$$h = \sum_{m=-j}^{j} \sqrt{(j+m)(j-m+1)}|j,m\rangle\langle j,m|, \tag{5}$$

where

$$r \in \mathbf{R}, \quad q = e^{2\pi i/(2j+1)}, \quad a \in \mathbf{R}. \tag{6}$$

It can be checked that the three operators

$$j_+ = hv_{ra}, \quad j_- = (v_{ra})^\dagger h, \quad j_z = \frac{1}{2}\left[h^2 - (v_{ra})^\dagger h^2 v_{ra}\right], \tag{7}$$

where $(v_{ra})^\dagger$ stands for the adjoint of v_{ra}, satisfy the commutation relations

$$[j_z, j_+] = +j_+, \quad [j_z, j_-] = -j_-, \quad [j_+, j_-] = 2j_z \tag{8}$$

of the algebra $su(2)$. (In angular momentum theory, the operators j_+ and j_- are connected to j^2 via $j^2 = j_\pm j_\mp + j_z(j_z \mp 1)$.)

The operator v_{ra} is unitary while the operator h is Hermitian. Thus, Eq. (7) corresponds to a polar decomposition of $su(2)$ with the help of the operators v_{ra} and h. It should be noted that v_{ra} can be derived in terms of operators acting on the tensor product of two commuting quon algebras associated with two truncated harmonic oscillators. The latter oscillators play a central role in the intoduction of k-fermions which are supersymmetric objects interpolating between fermions and bosons [20, 21].

It is evident that v_{ra} and j^2 commute. Therefore, the $\{j^2, v_{ra}\}$ scheme constitutes an alternative to the $\{j^2, j_z\}$ scheme. This yields the following result.

Result 1. *For fixed j, r and a, the $2j+1$ vectors*

$$|j\alpha; ra\rangle = \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} q^{(j+m)(j-m+1)a/2 - jmr + (j+m)\alpha}|j,m\rangle, \tag{9}$$

with $\alpha = 0, 1, \ldots, 2j$, are common eigenvectors of v_{ra} and j^2. The eigenvalues of v_{ra} are given by

$$v_{ra}|j\alpha; ra\rangle = q^{j(a+r)-\alpha}|j\alpha; ra\rangle, \tag{10}$$

so that the spectrum of v_{ra} is nondegenerate.

For fixed j, r and a, the inner product

$$\langle j\alpha; ra | j\beta; ra\rangle = \delta_{\alpha,\beta} \tag{11}$$

shows that $\{|j\alpha; ra\rangle : \alpha = 0, 1, \ldots, 2j\}$ is an orthonormal set which provides a nonstandard basis for the irreducible matrix representation of $SU(2)$ associated with j.

III. QUANTUM QUADRATIC DISCRETE FOURIER TRANSFORM

In view of the interest of the bases $\{|j\alpha; 0a\rangle : \alpha = 0, 1, \ldots, 2j\}$ for quantum information and quantum computation, we shall continue with the case $r = 0$. From now on, we shall also assume that $a = 0, 1, \ldots, 2j$. Furthermore, by making the following change of notation

$$n \equiv j + m, \quad |n\rangle \equiv |j, m\rangle, \quad d \equiv 2j + 1, \tag{12}$$

Eq. (9) gives

$$|j\alpha; 0a\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} q^{n(d-n)a/2+n\alpha} |n\rangle. \tag{13}$$

Alternatively, the change of notation

$$k \equiv j - m, \quad |k\rangle \equiv |j, m\rangle, \quad d \equiv 2j + 1 \tag{14}$$

leads to

$$|j\alpha; 0a\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} q^{(k+1)(d-k-1)a/2-(k+1)\alpha} |k\rangle. \tag{15}$$

Equations (13) and (15) were used in [22] and [23, 24]. They are equivalent as far as quadratic discrete Fourier transforms and mutually unbiased bases (MUBs) are concerned. Both Eqs. (13) and (15) correspond to quantum quadratic discrete Fourier transforms which can be inverted to give

$$|n\rangle = \frac{1}{\sqrt{d}} q^{-n(d-n)a/2} \sum_{\alpha=0}^{d-1} q^{-\alpha n} |j\alpha; 0a\rangle \tag{16}$$

and

$$|k\rangle = \frac{1}{\sqrt{d}} q^{-(k+1)(d-k-1)a/2} \sum_{\alpha=0}^{d-1} q^{\alpha(k+1)} |j\alpha; 0a\rangle. \tag{17}$$

Note that the word *quantum* in *quantum quadratic discrete Fourier transform* refers to the fact that the vectors $|n\rangle$ or $|k\rangle$ (corresponding to $|j,m\rangle$) are used in the quantum theory of generalized angular momentum.

In the following we shall adopt the change of notation (12) and shall re-define $|j\alpha;0a\rangle$ as $|a\alpha\rangle$. In other words

$$|a\alpha\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1} q^{n(d-n)a/2+n\alpha}|n\rangle \tag{18}$$

or, in an equivalent way,

$$|n\rangle = \frac{1}{\sqrt{d}} q^{-n(d-n)a/2}\sum_{\alpha=0}^{d-1} q^{-\alpha n}|a\alpha\rangle. \tag{19}$$

Note that the action of the operator v_{0a} on the vector $|n\rangle$ reads

$$v_{0a}|n\rangle = q^{-(n+1)a}|n+1\rangle \tag{20}$$

modulo d. It is clear that the basis

$$B_{0a} = \{|a\alpha\rangle : \alpha = 0,1,\ldots,d-1\} \tag{21}$$

is an alternative to the basis $B_d \equiv B_{2j+1}$. There are $d = 2j+1$ bases of this type for a in the ring $\mathbf{Z}/d\mathbf{Z}$. Each basis B_{0a} spans the regular representation of the cyclic group C_d.

IV. QUADRATIC DISCRETE FOURIER TRANSFORM

The expression

$$(H_{0a})_{n\alpha} = \frac{1}{\sqrt{d}} q^{n(d-n)a/2+n\alpha}, \tag{22}$$

occurring in (18), defines the $n\alpha^{\text{th}}$ matrix element of a quadratic discrete Fourier transform. To be more precise, for fixed d and a, let us consider the transformation

$$x = \{x(n) \in \mathbf{C} : n = 0,1,\ldots,d-1\} \leftrightarrow y = \{y(\alpha) \in \mathbf{C} : \alpha = 0,1,\ldots,d-1\} \tag{23}$$

defined by

$$y(\alpha) = \sum_{n=0}^{d-1} (H_{0a})_{n\alpha}\, x(n) \Leftrightarrow x(n) = \sum_{\alpha=0}^{d-1} \overline{(H_{0a})_{n\alpha}} y(\alpha). \tag{24}$$

The particular case $a = 0$ corresponds to the ordinary discrete Fourier transform which satisfies

$$(H_{00})^4 = I_d, \tag{25}$$

where I_d is the identity $d \times d$ matrix. For $a \neq 0$, the bijective transformation $x \leftrightarrow y$ can be thought of as a quadratic discrete Fourier transform. The analog of the Parseval-Plancherel theorem for the usual Fourier transform can be expressed in the following way.

Result 2. *The quadratic discrete Fourier transforms $x \leftrightarrow y$ and $x' \leftrightarrow y'$ associated with the same matrix H_{0a}, $a \in \mathbf{Z}/d\mathbf{Z}$, satisfy the conservation rule*

$$\sum_{\alpha=0}^{d-1} \overline{y(\alpha)} y'(\alpha) = \sum_{n=0}^{d-1} \overline{x(n)} x'(n), \tag{26}$$

where the common value is independent of a.

It is to be observed that the matrix H_{0a} is a generalized Hadamard matrix in the sense that the modulus of each of its matrix element is equal to $1/\sqrt{d}$. Such a matrix reduces the endomorphism associated with the operator v_{0a}. As a matter of fact, we have

$$(H_{0a})^\dagger V_{0a} H_{0a} = q^{(d-1)a/2} \begin{pmatrix} q^1 & 0 & \dots & 0 \\ 0 & q^2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & q^d \end{pmatrix}, \tag{27}$$

where the matrix

$$V_{0a} = \begin{pmatrix} 0 & q^a & 0 & \dots & 0 \\ 0 & 0 & q^{2a} & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & q^{(d-1)a} \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{28}$$

represents the linear operator v_{0a} on the basis

$$B_d = \{|n\rangle : n = d-1, d-2, \dots, 0\}, \tag{29}$$

known as the computational basis in quantum information and quantum computation.

The Hadamard matrices H_{0a} and H_{0b} ($a, b \in \mathbf{Z}/d\mathbf{Z}$) are connected to the inner product $\langle a\alpha|b\beta\rangle$. In fact, we have

$$\left((H_{0a})^\dagger\, H_{0b}\right)_{\alpha\beta} = \langle a\alpha|b\beta\rangle = \frac{1}{d}\sum_{n=0}^{d-1} q^{n(d-n)(b-a)/2+n(\beta-\alpha)}. \tag{30}$$

Thus, each matrix element of $(H_{0a})^\dagger\, H_{0b}$ can be written in the form of a generalized quadratic Gauss sum $S(u, v, w)$ defined by [25]

$$S(u, v, w) = \sum_{n=0}^{|w|-1} e^{i\pi(un^2+vn)/w}, \tag{31}$$

where u, v, and w are integers such that u and w are mutually prime, $uw \neq 0$, and $uw + v$ is even. In detail, we obtain

$$\langle a\alpha|b\beta\rangle = \left((H_{0a})^\dagger\, H_{0b}\right)_{\alpha\beta} = \frac{1}{d}S(u, v, w), \tag{32}$$

with the parameters

$$u = a - b, \quad v = -(a - b)d - 2(\alpha - \beta), \quad w = d, \tag{33}$$

which ensure that $uw + v$ is even.

The matrix V_{0a} can be decomposed as

$$V_{0a} = X_0 Z^a, \tag{34}$$

where

$$X_0 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{35}$$

and

$$Z = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & q & 0 & \dots & 0 \\ 0 & 0 & q^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & q^{d-1} \end{pmatrix}. \tag{36}$$

The unitary matrices X_0 and Z q-commute in the sense that

$$X_0 Z - qZX_0 = 0. \tag{37}$$

In addition, they satisfy

$$(X_0)^d = Z^d = I_d. \tag{38}$$

Equations (37) and (38) show that X_0 (to be noted as X in what follows in order to conform to the notations used for Pauli matrices) and Z constitute a Weyl pair. Weyl pairs were introduced at the beginning of quantum mechanics [26] and used for building operator unitary bases [12]. The Weyl pair (X, Z) turns out to be an integrity basis for generating a set $\{X^a Z^b : a, b \in \mathbf{Z}/d\mathbf{Z}\}$ of d^2 generalized Pauli matrices in d dimensions (see for instance [23, 24] and references therein). In this respect, note that for $d = 2$ we have

$$X = \sigma_x, \quad Z = \sigma_z, \quad XZ = -i\sigma_y, \quad X^0 Z^0 = \sigma_0, \tag{39}$$

in terms of the ordinary Pauli matrices $\sigma_0 = I_2$, σ_x, σ_y, and σ_z. Equations (37) and (38) can be generalized through

$$V_{0a} Z - qZV_{0a} = 0, \quad (V_{0a})^d = e^{i\pi(d-1)a} I_d, \quad Z^d = I_d, \tag{40}$$

so that other pairs of Weyl can be obtained from V_{0a} and Z.

V. MUTUALLY UNBIASED BASES

From a very general point of view, let us recall that two orthonormal bases $B_a = \{|a\alpha\rangle : \alpha = 0, 1, \dots, d-1\}$ and $B_b = \{|b\beta\rangle : \beta = 0, 1, \dots, d-1\}$ of the Hilbert space $\mathbf{C}^d$ are said to be mutually unbiased if and only if the inner product $\langle a\alpha|b\beta\rangle$ has a modulus independent of α and β. In other words

$$\forall \alpha \in \mathbf{Z}/d\mathbf{Z}, \forall \beta \in \mathbf{Z}/d\mathbf{Z} : |\langle a\alpha|b\beta\rangle| = \delta_{a,b}\delta_{\alpha,\beta} + (1 - \delta_{a,b})\frac{1}{\sqrt{d}}. \tag{41}$$

From Eq. (41), note that if two MUBs undergo the same unitary or antiunitary transformation, they remain mutually unbiased. It is well-known that the maximum number $\mathcal{N}$ of MUBs in $\mathbf{C}^d$ is $\mathcal{N} = 1 + d$ and that this number is attained when d is a prime number p or a power p^e ($e \geq 2$) of a prime number p [13]-[15]. In the other cases ($d \neq p^e$, p prime and e integer with $e \geq 1$), the number $\mathcal{N}$ is not known although it can be shown that $3 \leq \mathcal{N} \leq 1 + d$ (see for example [16]). In the general composite case $d = \prod_i p_i^{e_i}$, we know that $1 + \min(p_i^{e_i}) \leq \mathcal{N} \leq 1 + d$ (see for example [17]).

A. Mutually unbiased bases for d prime

For $d = 2$, it can be checked that the bases B_{00}, B_{01}, and B_2 are $1 + d = 3$ MUBs. A similar result follows for $d = 3$: the bases B_{00}, B_{01}, B_{02}, and B_3 are $1 + d = 4$ MUBs. This can be generalized by the following result.

Result 3. *For $d = p$, with p a prime number, the bases $B_{00}, B_{01}, \ldots, B_{0p-1}, B_p$ form a complete set of $1 + p$ MUBs. The p^2 vectors $|a\alpha\rangle$, with $a, \alpha = 0, 1, \ldots, p-1$, of the bases $B_{00}, B_{01}, \ldots, B_{0p-1}$ are given by a single formula (namely Eq. (18)).*

The proof of Result 3 is as follows. First, Eq. (18) yields

$$|\langle k|a\alpha\rangle| = \frac{1}{\sqrt{p}}, \tag{42}$$

a relation that holds for all k, a, and α in $\mathbf{Z}/p\mathbf{Z}$ so that each basis B_{0a} is unbiased with B_p. Second, the generalized quadratic Gauss sum $S(u, v, w)$ in (32), with $d = p$ prime, can be calculated to give

$$|\langle a\alpha|b\beta\rangle| = \frac{1}{\sqrt{p}}, \tag{43}$$

for all a, b, α, and β in $\mathbf{Z}/p\mathbf{Z}$. This completes the proof.

We note in passing that, in the case where $d = p$ is a prime integer, the product $(H_{0a})^\dagger H_{0b}$ is another generalized Hadamard matrix.

To close this subsection, we may ask what becomes Result 3 when the prime integer p is replaced by an arbitrary (not prime) integer d. In this case, the formula (18) does not provide a complete set of $1 + d$ MUBs. However, it is possible to show [23, 24] that the bases B_{0a}, $B_{0a\oplus 1}$, and B_d are three MUBs in $\mathbf{C}^d$ (the addition $\oplus$ is understood modulo d). This result is in agreement with the well-known result according to which the maximum number of MUBs in $\mathbf{C}^d$, with d arbitrary, is greater or equal to 3 ([16]). Moreover, it can be proved [23, 24] that the bases B_{0a} and $B_{0a\oplus 2}$ are unbiased for d odd with $d \geq 3$ (d prime or nor prime).

B. Mutually unbiased bases for d power of a prime

Equation (18) can be used for deriving a complete set of $1 + p^e$ MUBs in the case where $d = p^e$ is a power ($e \geq 2$) of a prime integer p. The general case is very much involved.

Hence, we shall proceed with the example $p = e = 2$ corresponding to two qubits.

For $d = 2^2 = 4$, the application of (18) and (21) yields four bases B_{0a} $(a = 0, 1, 2, 3)$. As a point of fact, the bases B_{00}, B_{01}, B_{02}, B_{03}, and B_4 do not form a complete set of $1 + d = 5$ MUBs. However, it is possible to construct a set of five MUBs from repeated application of (18).

Four of the five MUBs for $d = 4$ can be constructed from the direct products $|a\alpha\rangle \otimes |b\beta\rangle$ which are eigenvectors of the operators $v_{0a} \otimes v_{0b}$. Obviously, the set

$$B_{0a0b} = \{|a\alpha\rangle \otimes |b\beta\rangle : \alpha, \beta = 0, 1\} \tag{44}$$

is an orthonormal basis in $\mathbf{C}^4$. It is evident that B_{0000} and B_{0101} are two unbiased bases since the modulus of the inner product of $|0\alpha\rangle \otimes |0\beta\rangle$ by $|1\alpha'\rangle \otimes |1\beta'\rangle$ is

$$|\langle 0\alpha|1\alpha'\rangle\langle 0\beta|1\beta'\rangle| = \frac{1}{\sqrt{4}}. \tag{45}$$

A similar result holds for the two bases B_{0001} and B_{0100}. However, the four bases B_{0000}, B_{0101}, B_{0001}, and B_{0100} are not mutually unbiased. A possible way to overcome this no-go result is to keep the bases B_{0000} and B_{0101} intact and to re-organize the vectors inside the bases B_{0001} and B_{0100} in order to obtain four MUBs. We are thus left with four bases

$$W_{00} \equiv B_{0000}, \quad W_{11} \equiv B_{0101}, \quad W_{01}, \quad W_{10}, \tag{46}$$

which together with the computational basis B_4 give five MUBs. In detail, we have

$$W_{00} = \{|0\alpha\rangle \otimes |0\beta\rangle : \alpha, \beta = 0, 1\}, \tag{47}$$

$$W_{11} = \{|1\alpha\rangle \otimes |1\beta\rangle : \alpha, \beta = 0, 1\}, \tag{48}$$

$$W_{01} = \{\lambda|0\alpha\rangle \otimes |1\beta\rangle + \mu|0\alpha \oplus 1\rangle \otimes |1\beta \oplus 1\rangle : \alpha, \beta = 0, 1\}, \tag{49}$$

$$W_{10} = \{\lambda|1\alpha\rangle \otimes |0\beta\rangle + \mu|1\alpha \oplus 1\rangle \otimes |0\beta \oplus 1\rangle : \alpha, \beta = 0, 1\}, \tag{50}$$

where

$$\lambda = \frac{1 - i}{2}, \quad \mu = \frac{1 + i}{2} \tag{51}$$

and the vectors of type $|a\alpha\rangle$ are given by the master formula (18). As a résumé, only two formulas are necessary for obtaining the $d^2 = 16$ vectors $|ab; \alpha\beta\rangle$ for the bases W_{ab}, namely

$$W_{00}, W_{11} \ : \ |aa; \alpha\beta\rangle = |a\alpha\rangle \otimes |a\beta\rangle, \tag{52}$$

$$W_{01}, W_{10} \ : \ |aa \oplus 1; \alpha\beta\rangle = \lambda|a\alpha\rangle \otimes |a \oplus 1\beta\rangle + \mu|a\alpha \oplus 1\rangle \otimes |a \oplus 1\beta \oplus 1\rangle, \tag{53}$$

for all a, α, and β in $\mathbf{Z}/2\mathbf{Z}$.

It is to be noted that the vectors of the W_{00} and W_{11} bases are not intricated (i.e., each vector is the direct product of two vectors) while the vectors of the W_{01} and W_{10} bases are intricated (i.e., each vector is not the direct product of two vectors).

Generalization of (52) and (53) can be obtained in more complicated situations (two qupits, three qubits, ...). The generalization of (52) is immediate. The generalization of (53) can be achieved by taking linear combinations of vectors such that each linear combination is made of vectors corresponding to the same eigenvalue of the relevant tensor product of operators of type v_{0a}.

VI. MUTUALLY UNBIASED BASES AND UNITARY GROUPS

In the case where d is a prime integer or a power of a prime integer, it is known that the set $\{X^a Z^b : a, b = 0, 1, \ldots, d-1\}$ of cardinality d^2 can be partitioned into $1 + d$ subsets containing each $d - 1$ commuting matrices (cf. [15]). By way of illustration, for $d = p$ with p prime, the $1 + p$ sets of $p - 1$ commuting matrices are easily seen to be

$$\mathcal{V}_0 = \{X^0 Z^a : a = 1, 2, \ldots, p-1\}, \tag{54}$$

$$\mathcal{V}_1 = \{X^a Z^0 : a = 1, 2, \ldots, p-1\}, \tag{55}$$

$$\mathcal{V}_2 = \{X^a Z^a : a = 1, 2, \ldots, p-1\}, \tag{56}$$

$$\mathcal{V}_3 = \{X^a Z^{2a} : a = 1, 2, \ldots, p-1\}, \tag{57}$$

$$\vdots$$

$$\mathcal{V}_{p-1} = \{X^a Z^{(p-2)a} : a = 1, 2, \ldots, p-1\}, \tag{58}$$

$$\mathcal{V}_p = \{X^a Z^{(p-1)a} : a = 1, 2, \ldots, p-1\}. \tag{59}$$

Each of the $1 + p$ sets $\mathcal{V}_0, \mathcal{V}_1, \ldots, \mathcal{V}_p$ can be put in a one-to-one correspondance with one basis of the complete set of $1 + p$ MUBs. In fact, $\mathcal{V}_0$ is associated with the computational basis while $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_p$ are associated with the p remaining MUBs in view of

$$V_{0a} \in \mathcal{V}_{a \oplus 1}, \quad a = 0, 1, \ldots, p-1. \tag{60}$$

Keeping into account the fact that the set $\{X^a Z^b : a, b = 0, 1, \ldots, p-1\} \setminus \{X^0 Z^0\}$ spans the Lie algebra of $SU(p)$, we get the following result.

Result 4. *For $d = p$, with p a prime integer, the Lie algebra $su(p)$ of the group $SU(p)$ can be decomposed into a direct sum of $1 + p$ abelian subalgebras each of dimension $p - 1$, i.e.*

$$su(p) \simeq v_0 \uplus v_1 \uplus \ldots \uplus v_p \tag{61}$$

where the $1 + p$ subalgebras $v_0, v_1, \ldots, v_p$ are Cartan subalgebras generated respectively by the sets $\mathcal{V}_0, \mathcal{V}_1, \ldots, \mathcal{V}_p$ containing each $p - 1$ commuting matrices.

Result 4 can be extended when $d = p^e$ with p a prime integer and e an integer ($e \geq 2$): there exists a decomposition of $su(p^e)$ into $1 + p^e$ abelian subalgebras of dimension $p^e - 1$ [27]-[33] (see also [23, 24]).

VII. CLOSING REMARKS

MUBs prove to be useful in classical information theory (network communication protocols), in quantum information theory (quantum state tomography and quantum cryptography), and in the theory of quantum mechanics as for the solution of the Mean King problem and the understanding of the Feynman path integral formalism (see [23, 24] for an extensive list of references).

There exist numerous ways of constructing sets of MUBs. Most of them are based on discrete Fourier transform over Galois fields and Galois rings, discrete Wigner distribution, generalized Pauli operators, mutually orthogonal Latin squares, discrete geometry methods, angular momentum theory and Lie-like approaches. In many of the papers dealing with the construction of MUBs for d a prime integer or a power of a prime integer, the explicit derivation of the bases requires the diagonalisation of a set of matrices.

In the present paper, the generic formula (18) arises from the diagonalisation of a single matrix (the matrix V_{0a}), for the $\mathcal{N} = 1 + p$ MUBs corresponding to $d = p$ with p a prime integer. Repeated application (e times) of this formula can be used in the case where $d = p^e$ is the power of a prime integer. Results 1 and 3 of this paper concern the closed form formula (18). Its derivation is based on the master matrix V_{0a}. From V_{0a} we can deduce the Weyl pair (X, Z) through

$$X = V_{00}, \quad Z = (V_{00})^{\dagger} \, V_{01}. \tag{62}$$

The operators X and Z are known as the flip or shift and clock operators, respectively. For d arbitrary, they are at the root of the Pauli group, a finite subgroup of order d^3 of the group $SU(d)$, of considerable importance in quantum information and quantum computation (e.g., see [34]-[36] and references therein for recent geometrical approaches to the Pauli group). The Pauli group is relevant for describing quantum errors and quantum fault tolerance in quantum computation.

Acknowledgments

This paper is dedicated to the memory of Yurii Fedorovich Smirnov. It was presented at the 13th International Conference on Symmetry Methods in Physics (SYMPHYS-XIII) organized in memory of Prof. Yurii Fedorovich Smirnov by the Bogoliubov Laboratory of Theoretical Physics of the Joint Institute for Nuclear Research and the International Center for Advanced Studies at Yerevan State University (the conference was held in Dubna, Russia, 6-9 July 2009). The author acknowledges the Organizing Committee of SYMPHYS-XIII, especially George S. Pogosyan, for their kind invitation to participate to this interesting conference.

---

[1] D.T. Sviridov and Yu.F. Smirnov, Soviet. Phys. Doklady **13**, 565 (1968).

[2] C.V. Vonsovski, C.V. Grimailov, V.I. Tcherepanov, A.N. Meng, D.T. Sviridov, Yu.F. Smirnov, and A.E. Nikiforov, *Crystal-Field Theory and Optical Spectra of Partly Filled d Shell Transition Ions* (Nauka, Moscow, 1969).

[3] D.T. Sviridov, Yu.F. Smirnov, and V.N. Tolstoy, *Spektroskopiya Kristallov* (Akad. Nauk SSSR, Moscow, 1975).

[4] D.T. Sviridov, R.K. Sviridova, and Yu.F. Smirnov, *Optical Spectra of Transition-Metal Ions in Crystal* (Nauka, Moscow, 1976).

[5] D.T. Sviridov and Yu.F. Smirnov, *Teoriya Opticheskikh Spektrov Perekhodnykh Metallov* (Izd. Nauka, Moscow, 1977).

[6] M. Kibler, J. Molec. Spectrosc. **26**, 111 (1968).

[7] M. Kibler, Int. J. Quantum Chem. **3**, 795 (1969).

[8] M. Kibler, C.R. Acad. Sci. (Paris), Ser. B **268**, 1221 (1969).

[9] M.R. Kibler, Group theory around ligand field theory, in: *Group Theoretical Methods in Physics*, eds. R.T. Sharp and B. Kolman (Academic Press, New York, 1977).

[10] M.R. Kibler, Finite symmetry adaptation in spectroscopy, in: *Recent Advances in Group Theory and Their Application to Spectroscopy*, ed. J.C. Donini (Plenum Press, New York, 1979).

[11] M. Kibler and M. Daoud, Symmetry adaptation and two-photon spectroscopy of ions in molecular or solid-state finite symmetry, in: *Symmetry Methods in Physics*, eds. Yu.F. Smirnov and R.M. Asherova (Russian Federation Ministry of Atomic Energy – Institute of Physics and Power Engineering, Obninsk, 1992).

[12] J. Schwinger, Proc. Nat. Acad. Sci. USA **46**, 570 (1960).

[13] I.D. Ivanović, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[14] W.K. Wootters and B.D. Fields, Ann. Phys. (N.Y.) **191** 363 (1989).

[15] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[16] M. Grassl, Elec. Notes Discrete Math. **20**, 151 (2005).

[17] M. Aschbacher, A.M. Childs, and P. Wocjan, J. Algebr. Comb. **25**, 111 (2007).

[18] M.R. Kibler, Int. J. Mod. Phys. B **20**, 1792 (2006).

[19] M.R. Kibler and M. Planat, Int. J. Mod. Phys. B **20**, 1802 (2006).

[20] M. Daoud, Y. Hassouni, and M. Kibler, The k-fermions as objects interpolating between fermions and bosons, in: *Symmetries in Science X*, eds. B. Gruber and M. Ramek (Plenum Press, New York, 1998).

[21] M. Daoud, Y. Hassouni, and M. Kibler, Phys. Atom. Nuclei **61**, 1821 (1998).

[22] O. Albouy and M.R. Kibler, SIGMA **3**, 076 (2007).

[23] M.R. Kibler, J. Phys. A: Math. Theor. **41**, 375302 (2008).

[24] M.R. Kibler, J. Phys. A: Math. Theor. **42**, 353001 (2009).

[25] B.C. Berndt, R.J. Evans, and K.S. Williams, *Gauss and Jacobi Sums* (Wiley, New York, 1998).

[26] H. Weyl, *The Theory of Groups and Quantum Mechanics* (Dover Publications, New York, 1931).

[27] A.I. Kostrikin, I.A. Kostrikin, and V.A. Ufnarovskiĭ, Proc. Steklov Inst. Math. **158**, 105 (1981).

[28] A.I. Kostrikin, I.A. Kostrikin, and V.A. Ufnarovskiĭ, Sov. Math. Dokl. **24**, 292 (1981).

[29] A.I. Kostrikin, I.A. Kostrikin, and V.A. Ufnarovskiĭ, Sov. Math. Dokl. **25**, 2327 (1982).

[30] J. Patera and H. Zassenhaus, J. Math. Phys. **29**, 665 (1988).

[31] A.I. Kostrikin and P.H. Tiep, *Expositions in Mathematics*, vol. 15 (de Gruyter, Berlin, 1994).

[32] I. Bengtsson, *Preprint* arXiv:0610216 [quant-ph] (2006).

[33] P.O. Boykin, M. Sitharam, P.H. Tiep, and P. Wocjan, Quantum Inf. Comput. **7**, 371 (2007).

[34] H. Havlicek and M. Saniga, J. Phys. A: Math. Theor. **41**, 015302 (2008).

[35] M. Planat, A.-C. Baboin, and M. Saniga, Int. J. Theor. Phys. **47**, 1127 (2008).

[36] O. Albouy, J. Phys. A: Math. Theor. **42**, 072001 (2009).